ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Family Name: ....

First Name: ....

Section: ....

Cryptography and Security Course

(Crypto Part)

Midterm Exam

December 9th, 2005

This document consists of 8 pages.

Instructions

Electronic devices are *not* allowed.

Answers must be written on the exercises sheet.

This exam contains 1 exercise made of 8 questions.

Answers can be either in French or English.

Questions of any kind will certainly *not* be answered. Potential errors in these sheets are part of the exam.

You have to put your full name on *each* page.

From Cryptographic Hash Functions to Message Authentication Codes

This exercise shall introduce Message Authentication Codes (MAC) constructions based on iterated cryptographic hash functions, i.e., hash functions based on the Merkle-Damgård scheme.

Iterated Hash Functions

In this problem, we consider a cryptographic hash function $h : \mathcal{M} \to \mathcal{H}$, where $\mathcal{M} = \{0,1\}^N$ and $\mathcal{H} = \{0,1\}^n$. We will assume that h is based on the Merkle-Damgård scheme (see Figure 1). We denote by $f : \{0,1\}^n \times \{0,1\}^\ell \to \{0,1\}^n$ the compression function. Recall that in this construction the padding is mandatory and only depends on the length of the message.

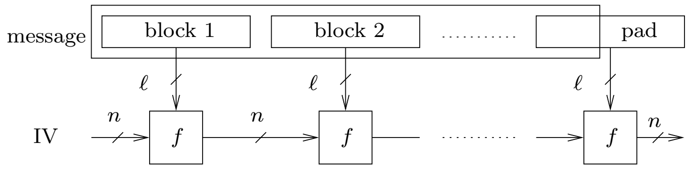

Figure 1: The Merkle-Damgård scheme

1. Give the name of two standard hash functions based on the Merkle-Damgård scheme. What is the the value of n and ℓ of these two hash functions?

2. Assuming that up to 2^{60} hash computations can be performed in a "reasonable" time, explain why n should be *at least* 128.

$\hookrightarrow$

$\hookleftarrow$

Message Authentication Codes

Alice wants to ensure the integrity and the authenticity of some information transmitted to Bob over an insecure channel. Assuming that she shares a common secret key k with Bob, a typical way of solving this problem is to use a *Message Authentication Code* (MAC) (see Figure 2). More precisely, denoting M the message she wants to send to Bob, Alice first computes an *authentication tag* $c = \mathrm{MAC}_k(M)$ using the secret key and then sends $c\|M$ to Bob (where $\|$ denotes the string concatenation). Bob will accept the tag and message $c'\|M'$ he receives only if $c' = \mathrm{MAC}_k(M')$.

The goal of a MAC is to prevent *forgery*: an adversary (with a limited computational power) should not be able to produce a valid authentication tag for a message not already sent by Alice or Bob (note that the key k is known by Alice and Bob *only*). In this problem, we will consider that the adversary has access to an oracle (i.e., a black box) which tells him, for any tag c and message M, whether $c = \mathrm{MAC}_k(M)$ or not (see Figure 3).

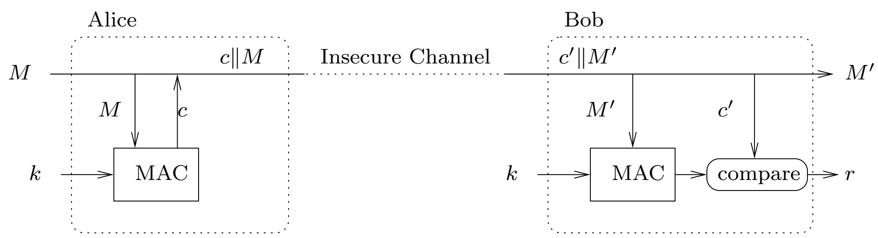

Figure 2: Authentication using a MAC

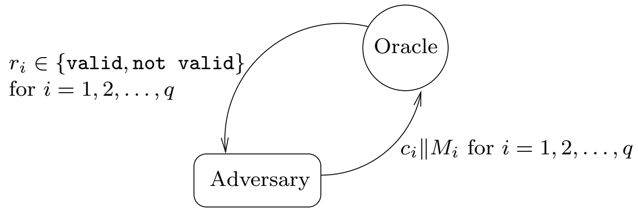

Figure 3: An Adversary learning whether $c_i = \mathrm{MAC}_k(M_i)$ for $i = 1, 2, \ldots, q$

3. We consider the case where $c \in \{0,1\}^{128}$ and $k \in \{0,1\}^{64}$. An adversary wants to produce a valid authentication tag for some (given) message M. Propose an algorithm which outputs $\mathrm{MAC}_k(M)$ with at most 2^{64} oracle queries.

4. We consider the case where $c \in \{0,1\}^{64}$ and $k \in \{0,1\}^{128}$. Once again, the adversary wants to produce a valid authentication tag for M. Propose another algorithm which outputs $\mathrm{MAC}_k(M)$ with at most 2^{64} oracle queries.

5. Considering the two previous questions, explain why it is not useful to have a key longer than the MAC output size. Explain why the length of c and k should be *at least* 64 bits.

Instead of using a standard MAC construction, Alice and Bob decide to compute a MAC based on an iterated hash function h such that for any message M

$$\mathrm{MAC}_k(M) = h(\widetilde{k} \| M), \text{ where } \widetilde{k} = \underbrace{k \| 00 \cdots 0}_{\ell \text{ bits}}.$$

6. Assume Alice sends one message M and its authentication tag $c = h(k\|M)$ to Bob over the insecure channel (so that the adversary knows M and c). Explain how the adversary can forge a valid tag $c' \neq c$ for a message M' longer than M.
Hint: Use the specific structure of Merkle-Damgård scheme.

$\hookrightarrow$

$\hookleftarrow$

Aware of the critical weakness of their construction, Alice and Bob decide to adopt the following construction for any message M:

$$\mathrm{MAC}_k(M) = h(M\|\widetilde{k}), \text{ where } \widetilde{k} = \underbrace{k\|00\cdots0}_{\ell \text{ bits}}.$$

7. Assume Alice has sent $2^{n/2}$ messages M_i and their authentication tags $c_i = h(M_i\|k)$ to Bob over the insecure channel. Explain how the adversary can forge a valid tag for a message $M' \neq M_i$ for all $i = 1, 2, \ldots, 2^{n/2}$ in roughly $2^{n/2}$ hash computations.
Hint: Use the Birthday paradox.

$\hookrightarrow$

8. Suggest a similar MAC construction (i.e., where the hash function is applied exactly once) immune to both previous attacks. Explain why your construction is secure.

$\hookleftarrow$